UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

FARHAD AZIMA, et. al.,	:	
	:	
	:	
Plaintiff	:	
	:	Civil Action No. 1:22-cv-08728 (PGG)
v.	:	
	:	
	:	
DECHERT LLP, et al.	:	
	:	
	:	
Defendants.	:	
	:	

DECLARATION OF SAMUEL ROSENTHAL IN SUPPORT OF DEFENDANT NICHOLAS DEL ROSSO AND VITAL MANAGEMENT SERVICES, INC.'S MOTION TO DISMISS

I, Samuel Rosenthal, hereby declare as follows:

1. I am the undersigned attorney for Defendants Nicholas Del Rosso ("Del Rosso") and Vital Management Services, Inc. ("Vital") (collectively, "Defendants") for the above captioned case. I make this declaration in support of Defendants' Motion to Dismiss. Except as otherwise stated, I have personal knowledge of the matters set forth herein.

2. Attached as Exhibit A is a true and correct copy of the Order issued and filed by the United States District Court of the Middle District of North Carolina in *Azima v. Del Rosso*, No. 1:20CV954, 2021 WL 5861282 (M.D.N.C.), on December 20, 2021.

3. Attached as Exhibit B is a true and correct copy of the original Complaint filed in *Azima v. RAK Investment Authority*, No. 1:16-cv-01948-KBJ (D.D.C.), on September 30, 2016, in the United States District Court for the District of Columbia.

4. Attached as Exhibit C is a true and correct copy of the Complaint filed in *Azima v. Del Rosso*, No. 1:20CV954, 2021 WL 5861282 (M.D.N.C.), on October 15, 2020, in the United States District Court for the Middle District of North Carolina.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on February 28, 2023, in Washington, D.C.

Dated: February 28, 2023
Washington, D.C.

Respectfully submitted,

/s/ *Samuel Rosenthal*

Samuel Rosenthal (Bar No. 329516)
Nelson Mullins Riley & Scarborough LLP
101 Constitution Ave., N.W., Suite 900
Washington, D.C. 20001
sam.rosenthal@nelsonmullins.com
Tel: 202-689-2915
Fax: 202-689-2860

Counsel for Defendants Nicholas Del Rosso and Vital Management Services, Inc.

EXHIBIT A

2021 WL 5861282
Only the Westlaw citation is currently available.
United States District Court, M.D. North Carolina.

Farhad AZIMA, Plaintiff,
v.
Nicholas DEL ROSSO and Vital Management Services, Inc., Defendants.

1:20CV954
|
Signed 12/10/2021

Attorneys and Law Firms

Christopher W. Jones, Jonathon D. Townsend, Ripley Rand, Womble Bond Dickinson (US) LLP, Raleigh, NC, Brian A. Hill, Calvin Lee, Ian A. Herbert, Kirby D. Behre, Miller & Chevalier Chartered, Washington, DC, for Plaintiff.

Brandon S. Neuman, Jeffrey M. Kelly, Kieran Joseph Shanahan, Nathaniel J. Pencook, Nelson Mullins Riley & Scarborough, LLP, Raleigh, NC, for Defendants.

MEMORANDUM OPINION AND ORDER

OSTEEN, JR., District Judge

***1** This matter is before this court for review of the Recommendation filed on August 9, 2021, by the Magistrate Judge in accordance with 28 U.S.C. § 636(b). (Doc. 54.) In the Recommendation, the Magistrate Judge recommends that Defendants Nicholas Del Rosso and Vital Management Services, Inc.'s ("Defendants") Motion to Dismiss, (Doc. 31), be denied in part as to Counts III, VIII, X, and XI of Plaintiff Farhad Azima's ("Plaintiff") Complaint but granted in part as to Plaintiff's other seven claims. (Doc. 54.) The Recommendation was served on the parties to this action on August 9, 2021, (Doc. 55). Both Plaintiff and Defendants filed timely objections to the Recommendation. (Docs. 56, 57.)

This court has appropriately reviewed the portions of the Recommendation to which objections were made and has made a de novo determination that the Magistrate Judge's Recommendation should be adopted in part and modified in part. This court finds Defendants' Motion to Dismiss as to Counts III and XI should be granted, contrary to the findings of the Recommendation. All other objections are overruled and the remainder of the Recommendation will be adopted.

I. FACTUAL AND PROCEDURAL BACKGROUND

This court fully adopts and incorporates the Magistrate Judge's Recommendation's factual and procedural case summary. (Recommendation (Doc. 54) at 2-4.) It recommended that seven of the eleven counts in the Complaint be dismissed. (Id. at 1.) The four remaining counts that it did not recommend dismissing, (together, the "Remaining Counts"), are for trade secret misappropriation under federal law (Count III), trade secret misappropriation under North Carolina law (Count VIII), civil conspiracy under North Carolina law (Count X), and invasion of privacy under North Carolina law (Count XI). (Id. at 38.)

On August 23, 2021, Plaintiff objected to the Magistrate Judge's recommendation that seven counts of the Complaint be dismissed. (Doc. 56.) Conversely, also on August 23, 2021, Defendants objected to the recommendation that the four Remaining Counts not be dismissed. (Doc. 57.) Both parties responded in opposition to the other's objection. (Docs. 58, 59.)

II. STANDARD OF REVIEW

This court is required to "make a de novo determination of those portions of the [Magistrate Judge's] report or specified proposed findings or recommendations to which objection is made." 28 U.S.C. § 636(b)(1)(c). This court "may accept, reject, or modify, in whole or in part, the findings or recommendations made by the [M]agistrate [J]udge.... or recommit the matter to the [M]agistrate [J]udge with instructions." Id.

III. ANALYSIS

This court has appropriately reviewed the portions of the Recommendation to which objections were made and has made a de novo determination as to each. This court concludes that the only objection meriting written analysis is Defendants' objection that a previous complaint filed by Plaintiff ought to be considered in evaluating whether Plaintiff's claims are time-barred by the statute of limitations. All other objections are rejected, as this court's determination on those issues is in accord with the Recommendation.

A. Whether the 2016 D.C. Complaint Should be Considered

***2** The Recommendation concluded that Plaintiff's September 2016 complaint filed in the United States District Court for the District of Columbia ("2016 D.C. Complaint") should not be considered in evaluating Defendants' statute of limitations affirmative defense. (Recommendation (Doc. 54) at 8-9.) In the 2016 D.C. Complaint, (Ex. 5 ("2016 D.C. Complaint") (Doc. 31-5)), Plaintiff accuses other parties — none of which are joined to this case — of orchestrating the hacking and publication of the hacked data. Thus, here, Defendants submitted the 2016 D.C. Complaint to establish that Plaintiff was sufficiently aware of this alleged wrongdoing to institute legal action by September 2016. (See Doc. 32 at 14—15, 17.) The 2016 D.C. Complaint alleges, inter alia, that:

> Based on the September 23, 2016, demand and threat letter from Defendant's counsel, and the disclosure of two websites by Defendant on September 29, 2016, it is clear that portions of the electronic data that had been hacked and misappropriated from Mr. Azima and his business associates on or about August 7, 2016, had been downloaded or transferred to remote websites known as "BitTorrent" sites and related micro-sites.

(2016 D.C. Complaint (Doc. 31-5) ¶ 18.) In the initial briefing before the Magistrate Judge, Plaintiff did not object to Defendants' proffering of the 2016 D.C. Complaint or to consideration of any of the allegations contained therein.

The Recommendation asserted that "for a statute-of-limitations defense to succeed at the motion to dismiss stage, 'all facts necessary to show the time bar must clearly appear on the face of the complaint.' " (Recommendation (Doc. 54) at 6 (some internal quotation marks omitted) (quoting Dickinson v. Univ. of N.C., 91 F. Supp. 3d 755, 763 (M.D.N.C. 2015)).) Thus, because Plaintiff's complaint does not mention the 2016 D.C. Complaint, the Magistrate Judge in the Recommendation found that it should not be considered. Defendants object, stressing that Plaintiff had never disputed that the "Court may take judicial notice of his 2016 complaint." (Defs.' Partial Obj. to Order and Recommendation on Defs.' Mot. to Dismiss Pursuant to Rule 12(b)(6) ("Defs.' Obj.") (Doc. 57) at 2, 6-14.)[1] Plaintiff opposes the objection. (Pl.'s Br. in Opp'n to Defs.' Objs. to Order and Recommendation ("Pl. Opp'n Br.") (Doc. 58) at 3-4.)

This court finds Defendants' objection should be sustained and that the 2016 D.C. Complaint should be considered at the motion to dismiss stage in evaluating Defendants' statute of limitations affirmative defense. The Recommendation correctly notes that "[g]enerally, an affirmative defense that a complaint is barred by a statute of limitations may not form the basis of [a] Rule 12(b)(6) dismissal unless all of the facts necessary for the defense appear on the face of the complaint." (Recommendation (Doc. 54) at 6-7 (quoting Morrison v. George E.B. Holding, No. 7:11-CV-168-BO, 2012 WL 1132787, at *3 (E.D.N.C. Apr. 4, 2012)).) However, the Recommendation neglected a key exception to that general rule repeatedly applied by courts in this circuit. See Morrison, 2012 WL 1132787, at *3; Mobley v. Estes, 1:17CV114, 2018 WL 704900, at *4 (M.D.N.C. Feb. 2, 2018). The exception holds that the general "face of the complaint" rule "[n]otwithstanding, the Court may also consider information in the public record when reviewing a motion to dismiss." Morrison, 2012 WL 1132787, at *3 (evaluating a statute of limitations affirmative defense); see also Mobley, 2018 WL 704900, at *4 (evaluating a statute of limitations affirmative defense and holding that "[g]enerally speaking, a court may not rely on extrinsic materials to adjudicate a motion to dismiss" but nevertheless "a court may properly take judicial notice of matters of public record." (citations and internal quotation marks omitted)).

***3** While the Fourth Circuit has evidently not addressed the specific issue of whether public records may be considered by the court when evaluating a statute of limitation affirmative defense at the motion to dismiss stage, other circuits have explicitly approved the practice. See, e.g., Ennenga v. Starns, 677 F.3d 766, 773-74 (7th Cir. 2012) (rejecting an argument that "the statute-of-limitations defense was not properly raised in a motion to dismiss because the defense was not plain on the face of the complaint," because "the court [properly] took judicial notice of the dates on which certain actions were taken ... in the earlier state-court litigation — facts readily ascertainable from the public court record"); Arbogast v. Kansas, 752 F. App'x 582, 584 n.1 (10th Cir.

2018); Staehr v. Hartford Fin. Servs. Grp., Inc., 547 F.3d 406, 425-26 (2d Cir. 2008). Moreover, the Fourth Circuit has expressly held that judicial notice of public records may be taken when evaluating motions to dismiss asserting res judicata affirmative defenses. Q Int'l Courier, Inc. v. Smoak, 441 F.3d 214, 216 (4th Cir. 2006); Andrews v. Daw, 201 F.3d 521, 524 n.1 (4th Cir. 2000).

Plaintiff argues that this Fourth Circuit precedent, such as Q International Courier, Inc. and Andrews, only allowed judicial notice of public records where the res judicata "defense raise[d] no disputed issue of fact." (Pl. Opp'n Br. (Doc. 58) at 4 (alteration in original) (emphasis removed) (internal quotation marks omitted) (quoting Q Int'l Courier, 441 F.3d at 216; Andrews, 201 F.3d at 524 n.1).) Plaintiff argues that in contrast, here, Defendants' statute of limitations "affirmative defense requires resolution of competing factual theories." (Id.) Therefore, Plaintiff argues judicially noticing a public record is inappropriate. (Id.) Plaintiff cites two cases to argue that the court "should allow discovery to resolve open factual questions rather than rely upon extrinsic documents to read inferences into the Complaint." (Id. (citing Waugh v. Elan Fin. Serv., Civil Action No. 3:17-4378, 2018 WL 2976430 (S.D. W. Va. June 13, 2018), and Khoja v. Orexigen Therapeutics, Inc., 899 F.3d 988 (9th Cir. 2018)).)

Neither case is relevant here. The first, Waugh, does not address the issue of judicial notice. The second, Khoja, is an out-of-circuit case that focuses on the risk of considering extrinsic documents in "SEC fraud matters, where there is already a heightened pleading standard, and the defendants possess materials to which the plaintiffs do not yet have access." Khoja, 899 F.3d at 998 (citations omitted). Here, Plaintiff's allegations do not face a heightened pleading standard nor do Defendants urge consideration of a document which Plaintiff cannot access – rather, Defendants seek to reference a publicly available record prepared for and filed on behalf of Plaintiff.

Therefore, consistent with the practice of courts in this circuit, e.g., Morrison, 2012 WL 1132787, at *3; Mobley, 2018 WL 704900, at *4, this court takes notice of the 2016 D.C. Complaint in adjudicating the statute of limitations affirmative defense asserted in Defendants' Motion to Dismiss. Importantly, this court's notice does not draw any conclusions as to whether the facts alleged in the 2016 D.C. Complaint are true or false. Instead, this court simply notices the existence of those factual allegations, which include that Plaintiff had been hacked and his hacked confidential business data posted online. (E.g., 2016 D.C. Complaint (Doc. 31-5) ¶¶ 10, 18.)

B. Whether the 2016 D.C. Complaint Establishes that the Remaining Counts are Time-Barred

The four Remaining Counts all have three-year statutes of limitations that accrue when the conduct underlying the respective count was apparent or discovered, or reasonably ought to have been apparent or discovered. (Recommendation (Doc. 54) at 7-8.) This court concludes that Plaintiff's factual allegations in the 2016 D.C. Complaint — that he had been hacked and his hacked confidential business data published online, (e.g., 2016 D.C. Complaint (Doc. 31-5) ¶¶ 10, 18) — establish that by 2016 Plaintiff had discovered the conduct underlying the Remaining Counts. Accordingly, the Remaining Counts' statutes of limitations seemingly accrued in 2016 and lapsed in 2019 — prior to this case's filing in 2020. Hence, Defendants insist that the Remaining Counts must be dismissed as time-barred.

***4** Plaintiff responds with four arguments why the Remaining Counts are not time-barred, even when the 2016 D.C. Complaint is considered. (Pl.'s Opp'n Br. (Doc. 58) at 6-9.) Three of those are unconvincing. The fourth, concerning Defendants' alleged 2018-2019 conduct, has merit. This court will address each argument in turn.

1. Knowledge of Defendants' Role

First, Plaintiff argues that "nothing in the 2016 lawsuit suggests that Azima was aware of Defendants' conduct in 2016; instead, Azima alleges in his Complaint that he 'did not learn of the role played by Del Rosso and Vital until recently[.]' " (Id. at 6 (quoting Complaint ("Compl.") (Doc. 1) ¶ 36).) That is irrelevant. None of the Remaining Counts' statutes of limitations make accrual contingent on when a plaintiff discovered (or should have discovered) a perpetrator's role, [2] but rather when the misappropriation or harm itself was discovered (or should have been discovered). See 18 U.S.C. § 1836(d) (Count III); N.C. Gen. Stat. § 66-157 (Count VIII); Sanders v. Gilchrist, No. 3:10cv68, 2011 WL 9374866, at *2 (W.D.N.C. Mar. 22, 2011) (Count X); Alexander v. City of Greensboro, No. 1:09-CV-293, 2011 WL

3360644, at *13 n.21 (M.D.N.C. Aug. 3, 2011) (citing N.C. Gen. Stat. § 1–52(16)) (Count XI).

2. Fraudulent Concealment and Equitable Estoppel [3]

***5** Next, Plaintiff argues that because the Complaint alleges that "Defendants took multiple steps to fraudulently conceal their involvement in hacking Azima.... Defendants should be [equitably] estopped from arguing that Azima's Complaint should be dismissed on statute of limitations grounds." (Pl.'s Opp'n Br. (Doc. 58) at 7-8.) Three of the Remaining Counts arise under North Carolina law (Counts VIII, X, and XI), and accordingly are subject to North Carolina tolling doctrines. (See Recommendation (Doc. 54) at 13.) To successfully toll these statutes of limitations via either equitable estoppel or fraudulent concealment [4] under North Carolina law, Plaintiff must establish that he relied on Defendants' conduct. (Id. at 14 n.4.) This court agrees with the Magistrate Judge's conclusion that Plaintiff has failed to do so. (Id. at 14-15 n.4.) Thus, neither equitable estoppel nor fraudulent concealment will toll the statutes of limitations for the three North Carolina law Remaining Counts.

The one other remaining count, Count III (misappropriation of trade secrets), arises under federal law. Hence, it is subject to federal tolling doctrines — most relevantly, fraudulent concealment and equitable estoppel. [5] See generally Edmonson v. Eagle Nat'l Bank, 922 F.3d 535, 559 (4th Cir. 2019). Neither are applicable here. Fraudulent concealment has three elements: "(1) the party pleading the statute of limitations fraudulently concealed facts that are the basis of the plaintiff's claim, and (2) the plaintiff failed to discover those facts within the statutory period, despite (3) the exercise of due diligence." Id. at 548 (quotation marks omitted) (quoting Supermarket of Marlinton, Inc. v. Meadow Gold Dairies, Inc., 71 F.3d 119, 122 (4th Cir. 1995)). Plaintiff cannot establish the second element because the 2016 D.C. Complaint's factual allegations demonstrate that during the statutory period Plaintiff discovered the supposedly concealed facts undergirding Count III. To toll the statute of limitations via federal equitable estoppel, a plaintiff must establish that "failure to timely file his claim derives ... from conduct taken by the defendant to induce the plaintiff not to timely file his claim." Id. at 549. In essence, a plaintiff must show reliance on a defendant's misconduct. As stated, supra Part III.B.1, this court agrees with the Magistrate Judge's conclusion that Plaintiff has not "alleged sufficient facts in his complaint to establish the element of reliance." (Recommendation (Doc. 54) at 15 (rejecting Plaintiff's invocation of equitable estoppel under North Carolina law).) Thus, Plaintiff has failed to establish the elements required for either fraudulent concealment or equitable estoppel to toll the statute of limitations for the remaining count arising under federal law.

3. Judicial Notice of Other Public Records

***6** Plaintiff argues that "if the Court accepts Defendants' argument that judicial notice is appropriate" for the 2016 D.C. Complaint, "the Court should then also take judicial notice of the public record referred to in Azima's previous filings." (Pl.'s Opp'n Br. (Doc. 58) at 9.) Plaintiff insists that these additional public records defeat Defendants' statute of limitations defense because they contain facts that show "Azima could not have been aware of [Defendants' violations] in 2016." (Id.) Specifically, Plaintiff urges the court to take notice of two matters of public record.

The first is "Del Rosso's first witness statement in the UK trial." (Id.) Plaintiff argues that this is relevant because it "shows the first time Azima learned that Del Rosso provided Azima's hacked data to Neil Gerrard and Dechert LLP." (Id.) Even if that is true, it is irrelevant to Defendants' statute of limitations defense. As explained, supra Part III.B.1, accrual for the Remaining Counts' statutes of limitations is not contingent on when Plaintiff learned of Defendants' roles in the alleged wrongdoing. Rather, accrual occurs when Plaintiff discovered the wrongdoing itself. Id. Thus, the Remaining Counts' statutes of limitations accrued in 2016 because the 2016 DC Complaint's allegations show Plaintiff had discovered the hacking and misappropriation by that time. Indeed, the 2016 D.C. Complaint even specifically alleges that Dechert had acquired Azima's hacked data. (E.g., 2016 D.C. Complaint (Doc. 31-5) ¶ 12.) That Plaintiff may not have uncovered Defendants' roles in that misappropriation until later, does not alter the accrual analysis. Therefore, this court declines to judicially notice Del Rosso's first U.K. trial witness statement because it is immaterial to Defendants' statute of limitations affirmative defense.

Plaintiff also urges this court to judicially notice that "during the pendency of the motion to dismiss, Del Rosso admitted to paying CyberRoot." (Pl.'s Opp'n Br. (Doc. 58) at 9.) That Del Rosso paid CyberRoot is alleged in Plaintiff's Complaint, (Compl. (Doc. 1) ¶ 5), and thus already assumed true for

the purposes of evaluating Defendants' Motion to Dismiss. Therefore, even if this court were to take the notice Plaintiff urges, it would have no bearing on this court's present analysis. Hence, this court declines to notice Del Rosso's alleged admission to paying CyberRoot.

4. Defendants' Alleged 2018-2019 Conduct

Plaintiff further argues that Defendants' alleged 2018-2019 conduct means the Remaining Counts are not time-barred, even considering the 2016 D.C. Complaint. Plaintiff insists that "the Complaint alleges multiple violations by Defendants independent of and long after the filing of the 2016 lawsuit." (Pl.'s Opp'n Br. (Doc. 58) at 7.) Specifically, Plaintiff stresses that "[t]he Complaint alleged that Defendants disclosed and used Azima's hacked data in 2018 and 2019." (Id. (citing Compl. (Doc. 1) ¶¶ 24, 26).) Plaintiff argues that "each disclosure in 2018 and 2019 was a separate violation of the" Remaining Counts, and "[t]hus, the statutes of limitation did not begin to run on those claims until at least 2018 or 2019, when the conduct occurred." (Id.) Therefore, "[j]udicial notice of the 2016 lawsuit could not have provided any information relevant to the statutes of limitation for Defendants' later conduct." (Id.)

***7** Defendants anticipated this argument and contend that "Azima's allegations simply do not link Defendants to the alleged 2018-19 conduct, so that conduct cannot be the basis for any claim against Defendants." (Defs.' Obj. (Doc. 57) at 18 n.6.) This court disagrees. For purposes of surviving a motion to dismiss, the Complaint sufficiently links Defendants to the 2018-2019 conduct. Critically, the Complaint alleges that

> Del Rosso hired the Indian hacking firm CyberRoot ....
>
> ....
>
> Acting at Defendants' direction, CyberRoot created, uploaded, and transmitted multiple unauthorized copies of Azima's data.... [A]t least some of that data was provided to Del Rosso ....
>
> ....
>
> CyberRoot created BitTorrent links that contained Azima's stolen data and those links were posted on the blog sites alleging fraud by Azima....
>
> ....
>
> In May and June 2018, the blog sites were modified to include new links to WeTransfer sites that contained copies of Azima's stolen data.
>
> CyberRoot regularly used WeTransfer links to transfer data to Vital....
>
> In June 2019, the links on the blog sites were modified to include new WeTransfer links containing some of Azima's stolen data.

(Compl. (Doc. 1) ¶¶ 16, 19, 22, 24-26.) At the motion to dismiss stage, these allegations - construed "in the light most favorable to the plaintiff" - more than "allow[ ] the court to draw the reasonable inference that" Defendants are sufficiently linked to the 2018-2019 conduct. (Recommendation (Doc. 54) at 4, 5, 34 (quoting Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc., 591 F.3d 250, 255 (4th Cir. 2009), and Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009)).)

a. Count XI (Invasion of Privacy under North Carolina Law)

However, this 2018-2019 conduct only relates to three of the four Remaining Counts. It does not relate to Count XI (invasion of privacy under North Carolina law). That invasion of privacy count is "tied to the actual hacking in 2016 (and not the subsequent dissemination of the data)." (See Recommendation (Doc. 54) at 16 n.5 (discussing Counts IV (computer trespass) and V (conversion)).) Therefore, because the 2018-2019 conduct does not relate to the invasion of privacy count and the 2016 D.C. Complaint shows that Plaintiff discovered the hacking in 2016, this court concludes that the invasion of privacy count accrued in 2016. Hence, its three-year statute of limitations lapsed in 2019, before this action was filed in 2020. Thus, Count XI must be dismissed as time-barred. This court will modify the Magistrate Judge's Recommendation that Defendants' Motion to Dismiss be denied as to Count XI and instead will grant the Motion to Dismiss as to Count XI.

b. Count III (Misappropriation of Trade Secrets under Federal Law)

***8** Even if the federal and state trade secret misappropriation counts (Counts III and VIII) are implicated by the 2018-2019 conduct, Defendants still maintain that dismissal is necessary. Defendants assert that "trade secrets claims accrue with the original incident," (Defs.' Obj. (Doc. 57) at 18 n.6), meaning that despite the later 2018-2019 conduct, these claims accrued in 2016 when the original misappropriation was discovered. This argument is valid as to the federal misappropriation count, Count III. That count's statute of limitations holds that "a continuing misappropriation constitutes a single claim of misappropriation." 18 U.S.C. § 1836(d). This means that:

> the first discovered (or discoverable) misappropriation of a trade secret commences the limitation period .... [A]lthough the initial wrongful acquisition of the trade secret and each subsequent misuse are separate acts of misappropriation, a claim for misappropriation arises only once ... at the time of the initial misappropriation, subject to the discovery rule.

B&P Littleford, LLC v. Prescott Mach., LLC, Nos. 20-1449/1451 2021 WL 3732313, at *6 (6th Cir. Aug. 24, 2021) (internal citations and quotation marks omitted); see also In re Outsidewall Tire Litig., Nos. 1:09cv1217/1218, 2010 WL 11474981, at *2 (E.D. Va. June 29, 2010) (interpreting Virginia's misappropriation of trade secret law's statute of limitations, which has the same "continuing misappropriation" language that the federal law has, and concluding that "the limitations period for claims alleging misappropriation of a single trade secret begins to run when the plaintiff discovers or reasonably should have discovered the first act of misappropriation, even if the misappropriation continues for an extended period of time"). Therefore, the new links to Plaintiff's data that were posted in 2018 and 2019 constituted a "continuing misappropriation" and thus did not re-accrue the statute of limitations for the federal misappropriation of trade secrets count. Rather, that count maintained an accrual date of 2016, when Plaintiff first discovered that links to his data had been posted — as alleged in the 2016 D.C. Complaint. Hence, the count's three-year statute of limitations lapsed in 2019, and Count III must be dismissed as time-barred. Therefore, this court will modify the Magistrate Judge's Recommendation that Defendants' Motion to Dismiss be denied as to Count III and instead will grant the Motion to Dismiss as to Count III.

c. Count VIII (Misappropriation of Trade Secrets under North Carolina Law)

In contrast to federal law, the North Carolina trade secret misappropriation law's statute of limitations does not include language addressing continuing misappropriations. See N.C. Gen. Stat. § 66-157. In lieu of such language, general North Carolina claim accrual doctrines apply. North Carolina law features a "continuing wrong" doctrine. Quality Built Homes, Inc. v. Town of Carthage, 371 N.C. 60, 70, 813 S.E.2d 218, 226 (2018). The North Carolina Supreme Court has described this doctrine as unexceptional and part of "the usual rules governing the operation of statutes of limitations." Id. North Carolina's continuing wrong doctrine holds that "the applicable limitations period starts anew in the event that an allegedly unlawful act is repeated." Id. Importantly, "the continuing wrong doctrine does not restart the statute of limitations period for earlier unlawful acts, it just provides that the limitations period starts anew for subsequently committed unlawful acts of the same nature." Lau v. Constable, No. 16 CVS 4393, 2019 WL 6051554, ¶ 34 (N.C. Super. Ct. Sept. 24, 2019); see also Sample v. Roper Lumber Co., 150 N.C. 161, 166, 63 S.E. 731, 732 (1909) ("[E]very wrong invasion of plaintiffs' property amounted to a distinct, separate trespass day by day, and for any and all such trespasses coming within the three years the defendant is responsible.").

Applying this doctrine to the original misappropriation of Plaintiff's trade secrets in 2016 and the more recent misappropriations in 2018-2019, "gives rise to multiple discrete claims corresponding to each act of misappropriation, and [b]ecause each act violates the law on its own, each act separately triggers its own limitations period." Heraeus Med. GmbH v. Esschem, Inc., 927 F.3d 727, 737 (3d Cir. 2019) (internal quotation marks omitted) (concluding that because Pennsylvania's misappropriation of trade secrets law's statute of limitations lacked language addressing "continuing misappropriations," each misappropriation started the limitations period anew). Therefore, for purposes of the North Carolina misappropriation of trade secrets count (Count VIII), the 2016, 2018, and 2019 conduct each separately triggered accrual of a respective three-year limitations period for that particular conduct. Consequently,

Plaintiff's 2020 filing of this case fell outside the three-year period for the 2016 conduct, but within the three-year period for the 2018-2019 conduct. Therefore, as to the 2018-2019 conduct, Count VIII is not time-barred. Thus, this court will ultimately accept, albeit for different reasons, the Magistrate Judge's recommendation that Defendants' Motion to Dismiss Count VIII be denied.

d. Count X (Civil Conspiracy under North Carolina Law)

***9** The final remaining count is for civil conspiracy under North Carolina law (Count X). "A claim for conspiracy ... cannot succeed without a successful underlying claim," Swain v. Elfland, 145 N.C. App. 383, 387, 550 S.E.2d 530, 534 (2001) (alteration in original) (quoting Jay Group, Ltd. v. Glasgow, 139 N.C. App. 595, 599, 534 S.E.2d 233, 236 (2000)). Therefore, here, the civil conspiracy claim only survives because this court has found that Count VIII (misappropriation of trade secrets under North Carolina law) remains viable, supra Part III.B.4.c. But, as "the statute of limitations for a civil conspiracy claim is governed by the underlying claim," Lau, 2019 WL 6051554, at *8 (citation omitted), Plaintiff's dependent civil conspiracy claim is likewise limited to the 2018-2019 conduct – the only allegations that are not time-barred. Thus, this court will ultimately accept, albeit for different reasons, the Magistrate Judge's recommendation that Defendants' Motion to Dismiss Count X be denied.

IV. CONCLUSION

For the foregoing reasons,

IT IS THEREFORE ORDERED that the Magistrate Judge's Recommendation, (Doc. 54), is **ADOPTED IN PART** and **MODIFIED IN PART.** The Magistrate Judge's Recommendation to deny Defendants' Motion to Dismiss Pursuant to Rule 12(b)(6), (Doc. 31), as to Counts III and XI is **MODIFIED** and instead the Motion to Dismiss as to Counts III and XI will be granted. The remainder of the Magistrate Judge's Recommendation is **ADOPTED**.

IT IS FURTHER ORDERED that Defendants' Motion to Dismiss Pursuant to Rule 12(b)(6), (Doc. 31), is **DENIED IN PART** as to Counts VIII and X of Plaintiff's Complaint but **GRANTED IN PART** as to Counts I, II, III, IV, V, VI, VII, IX, and XI.

IT IS FURTHER ORDERED that Plaintiff's Emergency Motion for Leave to File Supplemental Information Related to Objection to Recommended Ruling and for Leave to Commence Discovery in Light of Newly Discovered Evidence, (Doc. 61), is **DENIED**.

IT IS FURTHER ORDERED that Plaintiff's Motion for Leave to File Supplemental Information Related to Defendants' Opposition to Emergency Motion for Leave to File Supplemental Information, (Doc. 64), is **DENIED**.

This the 10th day of December, 2021.

All Citations

Slip Copy, 2021 WL 5861282

Footnotes

1 All citations in this Memorandum Opinion and Order to documents filed with the court refer to the page numbers located at the bottom right-hand corner of the documents as they appear on CM/ECF.

2 In contrast, the statutes of limitations for two counts that the Magistrate Judge recommended dismissing on other grounds — identity theft (Count VI) and publication of personal information (Count VII) — do make accrual so contingent. N.C. Gen. Stat. § 1-539.2C(c) ("Civil actions under this section must be brought within three years from the date on which the identity of the wrongdoer was discovered or reasonably should have been discovered." (emphasis added)).

3 After the parties had fully briefed their objections to the Recommendation, Plaintiff filed an "emergency motion" seeking leave to file supplemental evidence related to his fraudulent concealment argument. (Doc. 61.) The supplemental evidence Plaintiff seeks to file are (1) text messages allegedly sent in 2020 between Del Rosso and a Mr. Aditya Jain ("Jain"), (2) a commercial contract, and (3) a letter from Plaintiff's U.K. counsel. (Exs. 1—3 (Docs. 61-1 — 61-3).) Plaintiff also seeks leave to commence discovery early because this evidence allegedly evinces "exigent circumstances." (Doc. 61 at 7-8; accord Doc. 64 at 1.)

First, this court admonishes Plaintiff that "attempts to introduce new evidence after the magistrate judge has acted are disfavored." Galloway v. Rajjob, No. 1:20CV1033, 2021 WL 1248626, at *1 (M.D.N.C. Apr. 5, 2021) (internal quotation marks omitted) (quoting Caldwell v. Jackson, 831 F. Supp. 2d 911, 914 (M.D.N.C. 2010)). This court has repeatedly stated that it "is of the belief that untimely submission of evidence often serves to undermine the magistrate review process rather than illuminate the arguments already before the court." Kielbania v. Indian Harbor Ins. Co., No. 1:11CV663, 2012 WL 6554081, at *1 (M.D.N.C. Dec. 14, 2012); Universal Leather, LLC v. Koro AR, S.A, No. 1:12CV604, 2013 WL 12327585, at *2 (M.D.N.C. Sept. 30, 2013), vacated on other grounds, 773 F.3d 553 (4th Cir. 2014).

Second, even if the supplemental evidence had been timely submitted, there is no exception to the rule barring consideration of extrinsic materials when adjudicating a motion to dismiss under which the supplemental evidence may be considered. None of the evidence qualifies as a public record, cf., e.g., Morrison, 2012 WL 1132787, at *3, nor is any of it authenticated, cf., e.g., Sec'y of State For Defence v. Trimble Navigation Ltd., 484 F.3d 700, 705 (4th Cir. 2007) (Documents not attached to a complaint may be considered at the motion to dismiss stage if they are "integral to the complaint and authentic." (emphasis added)). As Defendants note, Plaintiff "does not provide any sworn statements authenticating these documents, as he has done in prior filings." (Doc. 62 at 9-10 (citing Doc. 25).) In response, Plaintiff filed yet another motion for leave, seeking to file U.K. court filings, which Plaintiff seems to believe authenticate the proffered text messages. (Doc. 64.) Leave will not be granted because the U.K. filings do no such thing. Instead, they merely establish that Del Rosso exchanged texts with Jain in 2020, (Doc. 64-1 ¶ 81(c); Doc. 64-2 ¶ 81(c)); they do not establish that those text messages include the particular messages proffered by Plaintiff here, (Doc. 61-1). In lieu of averments or other support credibly verifying, inter alia, the supplemental evidence's provenance, chain of custody, and date, this court finds that it remains unauthenticated. Therefore, because the supplemental evidence cannot be considered at this juncture, leave to file it will be denied. Accordingly, this court will deny as moot Plaintiff's corresponding request for early discovery.

4 The exact elements of North Carolina fraudulent concealment are murky, but "to the extent that fraudulent concealment has been recognized by North Carolina courts as a tolling doctrine, a plaintiff must still 'allege reliance on the defendant's misrepresentations or omissions.' " (Recommendation (Doc. 54) at 14-15 n.4 (quoting Wilkerson v. Christian, No. 1:06CV00871, 2008 WL 483445, at *12 (M.D.N.C. Feb. 19, 2008)).)

5 This court notes the existence of an additional similar tolling doctrine known as "equitable tolling." Edmonson, 922 at 551. However, unlike fraudulent concealment and equitable estoppel, equitable tolling does not require defendant misconduct. Id. at 449. Plaintiff's invocation of tolling doctrines is premised on Defendants' alleged misconduct, (Pl.'s Opp'n Br. (Doc. 58) at 7-8), and thus is more appropriately analyzed within "the domain of fraudulent concealment and equitable estoppel." Edmonson, 922 F.3d at 549 (quoting Shropshear v. Corp. Counsel of City of Chicago, 275 F.3d 593, 597 (7th Cir. 2001) (characterizing "tolling of the statute of limitations ... on the basis of defendant misconduct" as "the domain of fraudulent concealment and equitable estoppel")).

End of Document

EXHIBIT B

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

FARHAD AZIMA, 5921 Ward Parkway Kansas City, Missouri 64113, Plaintiff, v. RAK INVESTMENT AUTHORITY, Sheikh Muhammad Bin Salem Road/E11 Ras al-Khaimah, United Arab Emirates, Defendant.	Civil Action No. 1:16-cv-1948

COMPLAINT

Plaintiff Farhad Azima, by and through his undersigned counsel, files this Complaint against defendant RAK Investment Authority and alleges as follows:

INTRODUCTION

1. This matter arises out of the wrongful and tortious conduct of Defendant and its agents relating to the theft, conversion and improper use of the electronic data of Plaintiff for the purpose of extorting money from Plaintiff and inflicting unfair competitive injury on Plaintiff. As a direct and proximate result of the actions and omissions of Defendant and its agents, Plaintiff has suffered, and is continuing to suffer, substantial injury for which Plaintiff seeks monetary and injunctive relief against Defendant.

PARTIES

2. Plaintiff Farhad Azima ("Mr. Azima" or "Plaintiff") is a U.S. citizen who resides in Kansas City, Missouri. He has various business interests in the United States.

3. Defendant RAK Investment Authority ("RAKIA" or "Defendant") is an investment entity with its principal place of business in the Emirate Ras al-Khaimah in the United Arab Emirates. RAKIA is involved in commercial and investment activity around the world, and RAKIA competes in several respects with businesses owned and operated by Mr. Azima and his business interests.

JURIDICTION AND VENUE

4. This Court has subject matter jurisdiction over this case pursuant to 28 U.S.C. § 1331, 28 U.S.C. § 1332 and 28 U.S.C. § 1367.

5. Venue properly lies in this Court pursuant to 28 U.S.C. § 1391(b)(2) and 28 U.S.C. § 1391(b)(3) because a substantial part of the events or omissions giving rise to some or all of Plaintiff's claims occurred in this district and/or Defendant is subject to the Court's personal jurisdiction with respect to this case.

FACTS

6. In 2015, RAKIA asked Mr. Azima to assist RAKIA by mediating a dispute that existed between RAKIA and certain persons, including RAKIA's former chief executive officer. Mr. Azima agreed to assist RAKIA and, over the course of several months, met numerous times with RAKIA's representative and its counsel, Dechert LLP, in an effort to mediate a resolution of the dispute. Mr. Azima incurred significant time and expense in providing this assistance to RAKIA but has never been compensated or reimbursed by RAKIA as a mediator for his services or expenses.

7. Through Mr. Azima's efforts and assistance, RAKIA was able to reach a tentative settlement of the dispute with its former chief executive officer and the other persons involved in the dispute. Soon after, RAKIA and its counsel refused to continue with the settlement discussions. When the settlement discussions broke down, RAKIA and its agents, including its counsel, unfairly and without justification began to blame Mr. Azima for the lack of a settlement, despite the fact that Mr. Azima simply served as a mediator between the two sides.

8. After several intense discussions between Mr. Azima and RAKIA's representative and counsel, on or about July 23, 2016, RAKIA's counsel ominously threatened Mr. Azima that Mr. Azima would be "collateral damage" from actions RAKIA intended to take against its former chief executive officer. RAKIA's counsel refused Mr. Azima's request for notes that were taken at the July 23, 2016, meeting in which the threat was made against Mr. Azima.

9. After the termination of the settlement discussions, Mr. Azima learned that the computer systems used by the former chief executive officer of RAKIA had been hacked and his emails had been misappropriated without his consent or authorization.

10. Shortly after the July 23, 2016, threat by RAKIA's counsel, Mr. Azima also learned that computers in the United States used by Mr. Azima had been hacked and that a massive volume of emails and other electronic data of Mr. Azima and his business associates had been illegally misappropriated and stolen on or about August 7, 2016. On information and belief, the volume of electronic data that was hacked and stolen from Mr. Azima and his business associates was approximately 65 gigabytes (GB).

11. The nature and extent of the hacking and misappropriation strongly indicates that the person or persons who stole the electronic data were highly skilled technologically and employed sophisticated hacking methods.

12. On September 23, 2016, Mr. Azima's counsel in Washington, D.C. suddenly received an email from David Hughes of Dechert, LLP, RAKIA's counsel in London, England (hereinafter "Defendant's counsel"). Attached to the email from Defendant's counsel was a letter containing various exhibits.[1] In the letter, Defendant's counsel demanded that Mr. Azima pay $4,162,500 to RAKIA and an affiliate of RAKIA within seven (7) days. Defendant's counsel insisted that the payment should be made in U.S. dollars and should be deposited in a bank account titled "Dechert LLP USD Client A/c." Defendant's counsel based this demand on information that RAKIA had "recently obtained . . . via publically available internet sources." Defendant's counsel threatened that, if the payment was not received by the deadline, RAKIA would "issue court proceedings in London against Mr. Azima without further notice."

13. In his letter, Defendant's counsel included substantial and detailed information relating to Mr. Azima that Defendant's counsel asserted was derived from the "publically available internet sources." Additionally, Defendant's counsel attached to his letter copies of certain documents that he claimed had been obtained from the "publically available internet sources." Without knowing at this time whether any portions of such documents had been altered or manipulated by Defendant's counsel or others, a review of the attachments to Defendant's counsel's letter indicates that many of the documents appear to be copies of portions of the electronic data that had been hacked and misappropriated from Mr. Azima and his business associates on or about August 7, 2016. Based on the foregoing and other facts alleged herein, it appears highly likely that Defendant or someone acting for or on behalf of Defendant had been involved in the original hacking and misappropriation of the internal and confidential

[1] Given the inappropriate and improper nature of certain information in Defendant's counsel's letter, Mr. Azima has omitted the letter as an exhibit to the Complaint but will amend or supplement the Complaint with a copy of the letter if and when an appropriate sealing or protective order can be presented to and entered by the Court.

electronic data of Mr. Azima or, at a minimum, downloaded or directly accessed the information from the "publically available internet sources."

14. The documents attached to Defendant's counsel's letter include emails that are clearly confidential, and that are internal to Mr. Azima and his business associates, and could not be legitimately in the possession of any third party.

15. As an additional threat, Defendant's counsel stated in his September 23, 2016, letter that RAKIA "currently intends to seek advice from its US lawyers as to the possibility of raising its concerns about [Mr. Azima's alleged conduct] with the relevant US enforcement agency." This additional threat is or would be a violation of Rule 8.4(g) of the District of Columbia Bar's Rules of Professional Conduct, which deems it "professional misconduct" for an attorney to "[s]eek or threaten to seek criminal charges . . . solely to obtain an advantage in a civil matter." It is evident that, by making this threat, Defendant's counsel intended to coerce or influence Mr. Azima to transfer $4,162,500 to the bank account titled "Dechert LLP USD Client A/c" on or before September 30, 2016.

16. Mr. Azima's counsel subsequently received an additional copy of Defendant's counsel's demand and threat letter by an overnight service.

17. On September 28, 2016, Mr. Azima's counsel sent an email to Defendant's counsel asking to extend the arbitrarily imposed deadline in order to permit Mr. Azima sufficient time to review and respond to Defendant's letter until October 3, 2016, and requested that Defendant's counsel identify "the website(s) from which some of the materials you attach are located." In an email to Mr. Azima's counsel, on September 29, 2016, Defendant's counsel unreasonably and punitively rejected the extension request. With respect to the request for information regarding the electronic data on which Defendant's counsel based their September

23, 2016, demand and threat letter, which stated that the "[d]ocuments were obtained from a number of sites which included [two website links containing the word "torrent"]."[2] Defendant's counsel explained that he had been "advised [by some person] that these sites may contain viruses and should only be accessed with professional assistance."

18. Based on the September 23, 2016, demand and threat letter from Defendant's counsel, and the disclosure of two websites by Defendant on September 29, 2016, it is clear that portions of the electronic data that had been hacked and misappropriated from Mr. Azima and his business associates on or about August 7, 2016, had been downloaded or transferred to remote websites known as "BitTorrent" sites and related micro-sites. On information and belief, the emails and electronic data of RAKIA's former chief executive officer that had been hacked and misappropriated were also posted to the same type of websites.

19. On information and belief, BitTorrent sites are often used to provide a platform to download large files. These sites are sometimes referred to as the "Dark Web" as their content is not readily available to the public. It is commonly and widely known that BitTorrent sites often contain misappropriated files, such as pirated movies and other misappropriated data. It is also commonly known that the micro-sites associated with BitTorrent sites contain substantial malware and software viruses which could and would infect the computers and systems of anyone who accesses those sites.

20. On information and belief, stolen and misappropriated data is disaggregated across BitTorrent sites and related micro-sites, which makes it highly unlikely, if not impossible, for a legitimate business to know independently, and without involvement in the

[2] Given the harmful nature of these links, Mr. Azima has omitted the links from the Complaint but will amend or supplement the Complaint if and when an appropriate sealing or protective order can be presented to and entered by the Court.

misappropriation or without direction, that such data exist on websites or how to access such data. In other words, the average computer user would have to be "tipped off" that the data is hidden on the BitTorrent site or related micro-sites and would need specific information to navigate the websites in order to access the data on those websites.

21. Any legitimate business that received notice and direction from a third-party regarding the existence of certain data on BitTorrent sites and related micro-sites would or should know that such data had been misappropriated or stolen.

22. On information and belief, there is no normal or proper reason for a legitimate business to access BitTorrent sites or related micro-sites. In fact, most security software employed by legitimate businesses is designed to completely block users from accessing any BitTorrent sites or related micro-sites due to the security risk those sites pose.

23. On information and belief, any person or entity seeking to download data on a BitTorrent site or related micro-sites would need highly specialized software to download the data.

24. Following receipt of the letter from Defendant's counsel on September 23, 2016, an initial investigation has revealed that data on certain BitTorrent sites and related micro-sites, including the websites referenced by Defendant's counsel in his September 29, 2016 email, is, or was derived from, data that was hacked, stolen and misappropriated from Mr. Azima and his business associates on or about August 7, 2016, as alleged above. Data on those sites include emails that are clearly confidential, and that are internal to Mr. Azima and his business associates, and could not be legitimately in the possession of any third party. As with the attachments to the September 23, 2016, letter from Defendant's counsel, any person or entity on

the other side of a business dispute would recognize immediately that those emails should not be in the possession of any third party.

25. On information and belief, at least one of the websites that contains data hacked, stolen and misappropriated from Mr. Azima and his business associates is hosted on computer systems in Dubai, United Arab Emirates, and was obviously created to disparage and harm Mr. Azima.

26. As a direct and proximate result of the hacking and theft of the confidential and internal data of Mr. Azima and his business associates that occurred on or about August 7, 2016, as well as the allegations and threats made by RAKIA and its counsel, on September 23, 2016, relating to that stolen and misappropriated data, Mr. Azima has incurred and continues to incur costs and expenses investigating, analyzing and redressing the theft of the data. The theft of the data has also caused Mr. Azima to suffer various injuries and damages, including those resulting from the disruption of his business. The costs, expenses and damages that Mr. Azima has already incurred relating to and arising from the theft of data exceed one hundred thousand dollars ($100,000.00).

27. Based on the foregoing facts and circumstances, one or more of the following is true:

a. RAKIA, directly or through its agents, caused computers located in the United States containing the confidential, internal data of Mr. Azima and his business associates to be hacked and such data to be stolen and misappropriated without Mr. Azima's consent or permission.

b. RAKIA and its agents knew or should have known that the confidential, internal data of Mr. Azima and his business associates had been hacked and that such data had been stolen and misappropriated without Mr. Azima's consent or permission.

c. RAKIA and its agents caused misappropriated and stolen data of Mr. Azima and his business associates to be posted to and maintained on BitTorrent websites and related micro-sites.

d. RAKIA and its agents knew or should have known that misappropriated and stolen data of Mr. Azima and his business associates had been posted to and were being maintained on BitTorrent websites and related micro-sites.

e. RAKIA and its agents accessed and/or downloaded misappropriated and stolen data of Mr. Azima and his business associates from BitTorrent websites and related micro-sites knowing that such data had been misappropriated and stolen from Mr. Azima and his business associates without their consent or permission.

f. RAKIA and its agents, including Defendant's counsel, have knowingly, intentionally and deliberately used misappropriated and stolen data of Mr. Azima and his business associates to threaten, coerce and harm Mr. Azima personally and in his business.

COUNT I
(Violation of Computer Fraud And Abuse Act)
(18 U.S.C. § 1030, et seq.)

28. Plaintiff incorporates by reference, as if fully set forth herein, the allegations contained in paragraphs 1-27, above.

29. RAKIA, directly and/or through its agents, knowingly and intentionally caused computers in the United States containing the internal and confidential electronic data of Mr. Azima to be accessed and damaged in violation of the Computer Fraud and

Abuse Act, 18 U.S.C. § 1030(a)(5), by, among other things, hacking into those computers for the purpose of stealing and misappropriating the internal and confidential electronic data of Mr. Azima.

30. At the time of the violation, the computers that contained the internal and confidential electronic data of Mr. Azima and that were accessed and damaged were used in, or affected, interstate commerce.

31. Mr. Azima was directly and proximately injured by the violation of 18 U.S.C. § 1030(a)(5), including incurring costs and expenses to identify, investigate, analyze and address the violation. As of the filing hereof, such costs and expenses far exceed the minimum requirement set forth 18 U.S.C. § 1030(c)(4)(a)(i)(I).

32. The actions of RAKIA have directly and proximately caused Mr. Azima to suffer substantial injury and legally cognizable damages in an amount to be determined at trial.

33. In addition, as a result of the past and continuing violations, Mr. Azima has suffered, and will likely continue to suffer, certain irreparable harm to his person, reputation and business.

COUNT II
(Aiding and Abetting A Violation of Computer Fraud And Abuse Act)
(18 U.S.C. § 1030, et seq.)

34. Plaintiff incorporates by reference, as if fully set forth herein, the allegations contained in paragraphs 1-33, above.

35. RAKIA, directly and/or through its agents, knowingly and intentionally aided and abetted a person or persons to access and damage computers in the United States containing the internal and confidential electronic data of Mr. Azima in violation

of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5), by among other things, hacking into those computers for the purpose of stealing and misappropriating the internal and confidential electronic data of Mr. Azima.

36. At the time of the violation, the computers that contained the internal and confidential electronic data of Mr. Azima and that were accessed and damaged were used in, or affected, interstate commerce.

37. Mr. Azima was directly and proximately injured by the actions of RAKIA and/or its agents in aiding and abetting the violation of 18 U.S.C. § 1030(a)(5), including incurring costs and expenses to identify, investigate, analyze and address the violations. As of the filing hereof, such costs and expenses far exceed the minimum requirement set forth 18 U.S.C. § 1030(c)(4)(a)(i)(I).

38. The actions of RAKIA have directly and proximately caused Mr. Azima to suffer substantial injury and legally cognizable damages in an amount to be determined at trial.

39. In addition, as a result of the past and continuing violations, Mr. Azima has suffered, and will likely continue to suffer, certain irreparable harm to his person, reputation and business.

COUNT III
(Conversion)

40. Plaintiff incorporates by reference, as if fully set forth herein, the allegations contained in paragraphs 1-39, above.

41. RAKIA, directly and/or through its agents, knowingly and intentionally hacked, misappropriated, stole and/or improperly came into possession of the internal

and confidential electronic data of Mr. Azima and has exercised wrongful dominion and control over that data in violation of Mr. Azima's rights.

42. The tortious actions of RAKIA constitute the unlawful conversion of Mr. Azima's property.

43. RAKIA's tortious actions were taken and motivated by animus, ill-will and malice towards Mr. Azima and with the specific intent of harming Mr. Azima in his person and his business.

44. The tortious actions of RAKIA have directly and proximately caused Mr. Azima to suffer substantial injury and legally cognizable damages in an amount to be determined at trial.

45. In addition, as a result of the past and continuing tortious conduct by RAKIA, Mr. Azima has suffered, and will likely continue to suffer, certain irreparable harm to his person, reputation and business.

COUNT IV
(Aiding And Abetting Conversion)

46. Plaintiff incorporates by reference, as if fully set forth herein, the allegations contained in paragraphs 1-45, above.

47. RAKIA, directly and/or through its agents, knowingly and intentionally aided and abetted a person or persons to hack, misappropriate, steal and/or improperly came into possession of the internal and confidential electronic data of Mr. Azima and to exercise wrongful dominion and control over that data in violation of Mr. Azima's rights.

48. The tortious actions of RAKIA constitute the unlawful aiding and abetting of the conversion of Mr. Azima's property.

49. RAKIA's tortious actions were taken and motivated by animus, ill-will and malice towards Mr. Azima and with the specific intent of harming Mr. Azima in his person and his business.

50. The tortious actions of RAKIA have directly and proximately caused Mr. Azima to suffer substantial injury and legally cognizable damages in an amount to be determined at trial.

51. In addition, as a result of the past and continuing tortious conduct by RAKIA, Mr. Azima has suffered, and will likely continue to suffer, certain irreparable harm to his person, reputation and business.

COUNT V
(Unfair Competition And Extortion)

52. Plaintiff incorporates by reference, as if fully set forth herein, the allegations contained in paragraphs 1-51, above.

53. RAKIA, directly and/or through its agents, knowingly and intentionally engaged in improper and illegal conduct against Mr. Azima in order to gain an unfair advantage in business competition with Mr. Azima.

54. The actions of RAKIA and/or its agents included, without limitation, the use of threats and extortion in order to cause Mr. Azima to pay substantial amounts of money to RAKIA and/or its agents.

55. The tortious actions of RAKIA were taken and motivated by animus, ill-will and malice towards Mr. Azima and with the specific intent of harming Mr. Azima in his person and his business.

56. The tortious actions of RAKIA have directly and proximately caused Mr. Azima to suffer substantial injury and legally cognizable damages in an amount to be determined at trial.

57. In addition, as a result of the past and continuing tortious conduct by RAKIA, Mr. Azima has suffered, and will likely continue to suffer, certain irreparable harm to his person, reputation and business.

PRAYER FOR RELIEF

On the basis of the foregoing, and such additional evidence as Plaintiff will present at trial, Plaintiff Farhad Azima requests the entry of judgment in his favor and against Defendant RAK Investment Authority on all counts of the Complaint and the award of the following relief:

1. All statutory and compensatory damages incurred by Plaintiff as a result of the violations of 18 U.S.C. § 1030, et seq., as alleged above, in an amount to be determined at trial.

2. Compensatory damages incurred by Plaintiff as a result of the actions of Defendant and its agents, in an amount to be determined at trial.

3. Punitive damages in an amount not less than Twenty Million Dollars ($20,000,000.00).

4. A mandatory injunction requiring Defendant and its agents to return to Plaintiff all electronic data and other property of Plaintiff that are in the possession, custody or control of Defendant and its agents.

5. A prohibitory injunction obligating Defendant and its agent to refrain in the future from misappropriating or otherwise accessing Plaintiff's internal and confidential electronic data or other property.

6. Pre-judgment and post-judgment interest in the amounts and at the rates provided by law.

7. The costs and expenses, including reasonable attorney's fees, incurred by Plaintiff in this action and as a result of the actions of Defendant and its agents alleged herein.

8. Such other and further relief as the Court deems just and proper.

Dated: September 30, 2016

Respectfully submitted,

/s/ Kirby D. Behre

Kirby D. Behre (D.C. Bar # 398461)
Timothy O'Toole (D.C. Bar # 469800)
Charles F. McAleer (D.C. Bar # 388681)
Miller & Chevalier Chartered
900 16th Street, NW
Washington, D.C. 20006
Tel: (202) 626-5800
Fax: (202) 626-5801
Email: kbehre@milchev.com
Email: totoole@milchev.com
Email: cmcaleer@milchev.com

EXHIBIT C

UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA
CASE NO. 20-cv-954

FARHAD AZIMA,

Plaintiffs,

v.

NICHOLAS DEL ROSSO and VITAL MANAGEMENT SERVICES, INC.,

Defendants.

COMPLAINT

Plaintiff, Farhad Azima, by and through his undersigned counsel, files this Complaint against Nicholas Del Rosso ("Del Rosso") and Vital Management Services Inc. ("Vital"; collectively, "Defendants"), and alleges as follows:

INTRODUCTION

1. Defendants Del Rosso and Vital oversaw and directed the hacking of Plaintiff Farhad Azima. Defendants stole Azima's computer data, including emails and trade secrets. The stolen data was then published online and used by Defendants and others, on behalf of the Ras Al Khaimah Investment Authority ("RAKIA"), in an attempt to ruin Azima's reputation and damage him financially. Upon information and belief, Defendants were engaged and paid by Dechert LLP, which represented RAKIA in a dispute with Azima.

2. RAKIA, the state investment entity for the government of Ras Al Khaimah, hired individuals and companies, directly and through Dechert LLP, to investigate Azima,

hack his computers, steal his private data, and weaponize that data in an attempt to ruin Azima. Those individuals and companies included Stuart Page in the United Kingdom and the Defendants in the United States. Defendant Vital was hired by Dechert LLP through partner Neil Gerrard on behalf of RAKIA, and Defendants then hired CyberRoot Risk Advisory Private Limited ("CyberRoot") to provide the technical support necessary to hack Azima. CyberRoot is a company based out of Gurgaon, India that engages in illegal hacking.

3. BellTroX Info Tech Services ("BellTroX") assisted CyberRoot in hacking Azima. BellTroX is a hacking company based in New Delhi, India. According to a June 9, 2020, press report by Thomson Reuters, BellTroX was involved in "one of the largest spy-for-hire operations ever exposed," helping clients spy on more than 10,000 email accounts over a period of seven years. On February 11, 2015, the founder and owner of BellTroX, Sumit Gupta, was indicted by the United States Department of Justice in the Northern District of California for hacking. Gupta remains at large.

4. In its investigation of 'hack-for-hire' organizations (including BellTroX), Thomson Reuters reviewed a cache of data revealing "tens of thousands of malicious messages designed to trick victims into giving up their passwords" – phishing and spear phishing emails – that BellTroX distributed between 2013 and 2020. Upon information and belief, the data cache revealed that email accounts belonging to Azima and his associates were among the accounts targeted by the BellTrox/CyberRoot phishing operation.

5. Defendants paid CyberRoot more than $1 million for the hacking of Azima and the dissemination of his stolen data.

6. At the direction of Del Rosso and Vital, CyberRoot sent Azima phishing and spear-phishing emails, and successfully induced Azima to unwittingly provide them with passwords for his accounts. The successful hack gave CyberRoot persistent access to Azima's computers and email accounts, and CyberRoot obtained real time access to Azima's emails. CyberRoot disclosed Azima's stolen data on internet blog sites they created. These blog sites contained links to BitTorrent sites and We Transfer sites, set up by CyberRoot, that contained at least some of the data Defendants and CyberRoot stole from Azima. The work done by CyberRoot, assisted by Bell TroX, was done at the direction of the Defendants and others.

7. Defendants hacked Azima because they were hired to do so on behalf of RAKIA by Gerrard and Dechert LLP. Dechert LLP represented RAKIA in a dispute with Azima, and Gerrard wanted Azima's stolen data to use in a suit to be brought by RAKIA against Azima in England. Page, Del Rosso, Gerrard, and RAKIA's manager James Buchanan created a false evidentiary trail to cover up their and RAKIA's responsibility for the hacking, and to suggest that Page had innocently found the hacked material on BitTorrents. RAKIA brought the lawsuit against Azima using the hacked material. The hacking was a defense raised by Azima, as well as forming the basis for a counterclaim by Azima.

8. The English court ruled that RAKIA, Page, and others had lied about how they obtained Azima's stolen data. Del Rosso gave a sworn witness statement in the U.K. suit, denying any knowledge of how the stolen emails were obtained. That witness statement was false. Del Rosso gave live, sworn testimony during the trial. That testimony was false as well. RAKIA's lawyers, including Dechert LLP, had also asserted (in formal correspondence, witness evidence and pleadings signed by those lawyers) that RAKIA had innocently discovered the materials on the internet. Those assertions were also false, given the Judge's ruling.

9. As a result of the conduct of Del Rosso, Vital, and their co-conspirators, Azima has suffered significant financial and reputational damage.

PARTIES

10. Plaintiff Farhad Azima is a U.S. citizen who resides and works in Kansas City, Missouri. He is a successful businessman who has owned and operated multiple aviation-related companies. Azima's businesses engage in interstate and foreign commerce. All of Azima's computers and servers were and are located in the United States.

11. Defendant Nicholas Del Rosso is the owner and sole employee of his company, Defendant Vital Management Services Inc. ("Vital"). Vital purports to provide investigative services, but it is not licensed as a private investigator in North Carolina. Vital is located at 1340 Environ Way, Chapel Hill, North Carolina, 27517, and Del Rosso lives at 318 Lystra Preserve Drive, Chapel Hill, North Carolina 27517.

12. Defendant Del Rosso is the president and owner of Vital, and he is one of two shareholders of Vital, along with his wife.

FACTS

13. Dechert LLP and partner Neil Gerrard hired Del Rosso and Vital to "investigate assets potentially stolen from the Government of Ras Al Khaimah ("RAK")." Throughout the course of his work for Dechert LLP, which lasted from at least August 2014 until at least 2019, Del Rosso was hired by Dechert LLP and Gerrard. Del Rosso communicated with lawyers from Dechert LLP on a "very regular basis." Del Rosso hired Chris Swecker, a North Carolina-based lawyer, to assist Defendants in their work for Gerrard and Dechert LLP.

The Hacking of Azima at Del Rosso's Direction

14. Starting in early 2015, Gerrard, Page, Buchanan, and others agreed to attack Azima. The agreement is evidenced by a redacted internal "Project Update" report dated March 26, 2015, presented by Page to the Ruler of RAK and provided to Buchanan and others, as well as numerous emails between Gerrard, Buchanan, and their associates, some of which discussed the plan to "target," "attack," and "go after" Azima using "another channel." Based on these emails, an English court concluded that the desire to attack Azima in the summer of 2015 "is clear." The Project Update report claimed Azima was part of a "US team" to publicize human rights abuses by RAK and Gerrard. The report stated that "[t]he campaign is not public yet, so we will be able to gather intelligence on their progress in order to monitor their activities and attempt to contain or ruin their plans." Gerrard admitted to reading this report.

15. Gerrard hired Del Rosso and Vital. Upon information and belief, Del Rosso was hired to target Azima and to obtain Azima's emails and confidential data, as well as for other purposes; and Page was retained to assist in the targeting of Azima, which upon information and belief included hacking Azima.

16. Del Rosso hired the Indian hacking firm CyberRoot to provide the technical expertise to attempt to lure Azima into providing his login data, so that Defendants and their co-conspirators could have persistent access to Azima's accounts and computers. At least five employees of CyberRoot, including one of the company's directors, Vibhor Sharma, hacked Azima pursuant to Del Rosso's instructions. CyberRoot was assisted by BellTroX, which permitted CyberRoot to use BellTroX's infrastructure, including its server, to conduct the hacking. This work was done at the direction of the Defendants and others. CyberRoot and BellTroX share common employees. One such employee is Preeti Thapiyal, whose LinkedIn page lists his work as including the creation of "undetectable phishing Payloads."

17. CyberRoot, assisted by BellTroX, attempted to gain access to Azima's computers and accounts through phishing and spear-phishing emails. They sent Azima phishing emails to harvest his credentials and gain access to his email accounts and computers. Azima complied, and unwittingly enabled CyberRoot's hackers to gain access to Azima's email accounts and computers. The breach of Azima's computer systems gave CyberRoot covert and persistent access to Azima's email accounts and computers.

18. Del Rosso, Vital, CyberRoot, and other co-conspirators, including Dechert LLP, Gerrard, and Page, obtained numerous confidential and protected trade secrets belonging to Azima and his companies, including but not limited to privileged and confidential legal communications and advice and confidential internal pricing lists relating to food transport for U.S. troops in Afghanistan.

The Disclosure of Azima's Stolen Data at Del Rosso's Direction

19. Acting at Defendants' direction, CyberRoot created, uploaded, and transmitted multiple unauthorized copies of Azima's data. Upon information and belief, at least some of that data was provided to Del Rosso, who was located in North Carolina.

20. In late July 2016, Gerrard met with Azima and threatened him. Within days of Gerrard's meeting with Azima, CyberRoot, which was assisted by BellTroX, created blog sites on or about August 7, 2016, accusing Azima of fraud. During this same period, Del Rosso made significant payments to CyberRoot for their efforts.

21. The websites contained links to BitTorrent sites that Dechert LLP later admitted contained large quantities of Azima's stolen data. These BitTorrent links were posted by users named anjames and an_james. The usernames anjames and an_james are usernames associated with Sharma at CyberRoot. CyberRoot also used the email account an_james@protonmail.ch to create these blog sites and upload Azima's stolen data.

22. CyberRoot posted the data on the internet to create the misimpression that the data CyberRoot and Defendants stole from Azima were available to anyone who used the internet. CyberRoot created BitTorrent links that contained Azima's stolen data and those

links were posted on the blog sites alleging fraud by Azima. Page, Del Rosso, Gerrard, and an Israeli journalist, Majdi Halabi, created a false story and evidentiary trail to cover up their and RAKIA's responsibility for the hacking, and to suggest that Page had innocently found the hacked material on BitTorrents after being alerted to it by Halabi.

23. In fact, the data on the BitTorrent links were not accessible to the public because the "seeders"[1] necessary for the data to be downloaded were not available. Dechert LLP, and others acting at their direction, are the only persons or entities known to have obtained the data from the BitTorrent sites.

24. In May and June 2018, the blog sites were modified to include new links to WeTransfer sites that contained copies of Azima's stolen data.

25. CyberRoot regularly used WeTransfer links to transfer data to Vital. CyberRoot set up the WeTransfer account using the email account an_james@protonmail.ch.

26. In June 2019, the links on the blog sites were modified to include new WeTransfer links containing some of Azima's stolen data. These links, as with all the links to copies of Azima's stolen data, were not authorized by Azima.

27. Defendants were engaged by Dechert LLP on behalf of RAKIA. Upon information and belief, Defendants were paid by Dechert LLP, directly or indirectly, for their work.

[1] A torrent seeder is a user who owns the file being made available online through the torrent system. Without a seeder, a file cannot be downloaded.

28. Upon information and belief, Dechert LLP paid Defendants more than $1 million.

29. Defendants paid CyberRoot more than $1 million.

30. Those payments were for CyberRoot's hacking services and the distribution of Azima's stolen data.

31. At least some of the payments made by Vital were sent to CyberRoot's bank, Kotak Mahindra Bank.

32. Substantial payments were made to CyberRoot around the time that Azima's stolen data was published online in August and September 2016.

Lawsuit Against Azima and False Testimony About Discovery of Azima's Data

33. In September 2016, Dechert LLP partner David Hughes, on RAKIA's behalf, threatened to file a lawsuit in the U.K. against Azima and provided Azima's counsel with some of the emails that Defendants and CyberRoot stole from Azima. RAKIA, represented by Dechert LLP, sued Azima in England in September 2016 repeatedly relying on the data that Defendants stole from Azima.

34. Prior to and during the January 2020 trial in the U.K., Dechert LLP and RAKIA repeatedly changed their stories about how Azima's stolen data was obtained. The English court ruled that the story put forward by RAKIA and others on their behalf about how they discovered the stolen data was false. Specifically, the court said that the story told by Page, Halabi, and others of innocent discovery of Azima's stolen data was "not true," involved "unexplained contradictions, inconsistencies, and implausible elements," and "was both

internally inconsistent and inconsistent with the contemporaneous documents."[2] The English court said that "the true facts" about how Dechert LLP and others obtained Azima's stolen data still "have not been disclosed," despite them being required to do so. The untrue story of innocent discovery was advanced by RAKIA's agents. Former Dechert LLP partner Hughes signed a statement of truth for RAKIA advancing the story of innocent discovery. Others, including Gerrard, Buchanan, and Page, put forward witness statements and testimony that supported the story the court found to be untrue.

35. Del Rosso was an important part of RAKIA's false story of "innocent discovery" by Page of Azima's stolen data. For example, Gerrard and Del Rosso exchanged a series of emails on August 15 and 16, 2016, in which Gerrard purported to "break the news" of the discovery of the hacked material on websites. But other evidence showed that Del Rosso was aware of these websites at least a week earlier. The emails of August 15 and 16, 2016, between Gerrard and Del Rosso were clearly an attempt to lay a false "paper trail" of discovery.

36. In his witness statement, Del Rosso hid his engagement of CyberRoot and denied any involvement in the hacking. Because of Del Rosso's concealment of the true facts, of which he had knowledge, Azima did not learn of the role played by Del Rosso and Vital until recently.

[2] *Ras Al Khaimah Investment Authority v. Farhad Azima*, [2020] EWHC 1327 (Ch).

JURISDICTION

37. This Court has federal question subject matter jurisdiction pursuant to 28 U.S.C. § 1331. Some of Azima's claims arise under federal law, including the Wiretap Act (Counts 1 and 2) and misappropriation of trade secrets under the Defend Trade Secrets Act and the Economic Espionage Act (Count 3).

38. The Court has supplemental jurisdiction pursuant to 28 U.S.C. § 1367 over Azima's other claims, since those other claims relate to the federal statutory claims in this action and form part of the same case or controversy under Article III of the United States Constitution.

39. Additionally, this Court has diversity subject matter jurisdiction pursuant to 28 U.S.C. § 1332 because Azima and Defendants are from different states and the amount in controversy exceeds $75,000, exclusive of interest and costs.

40. The Court's jurisdiction over defendants comports with due process. The Court has personal jurisdiction over Defendants Del Rosso and Vital, who are domiciled or have their principal place of business in North Carolina. Del Rosso works at Vital in North Carolina and lives at 318 Lystra Preserve Drive, Chapel Hill, North Carolina 27517. Vital is based in North Carolina and is located at 1340 Environ Way, Chapel Hill, North Carolina, 27517.

VENUE

41. Venue is proper under 18 U.S.C. § 1965(a) because the Defendants transact their affairs in this Judicial District. Defendants Del Rosso and Vital both transact their

affairs in Chapel Hill, North Carolina, with Azima's causes of action arising out of those North Carolina transactions.

42. Venue is also proper under 28 U.S.C. § 1391(b)(2) because this is a judicial district in which a substantial part of the events or omissions giving rise to the claim occurred. Defendants conspired with others and coordinated their illegal campaign to hack Azima and publish his stolen data from their principal place of business in Chapel Hill, North Carolina.

43. Venue is also proper under 28 U.S.C. § 1391(b)(3) because this judicial district has personal jurisdiction over all defendants.

COUNT ONE (All Defendants)

I. Disclosure of Wire, Oral, or Electronic Communications under the Wiretap Act (18 U.S.C. §§ 2511(1)(c) and 2520)

44. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

45. It is a violation of 18 U.S.C. § 2511(c) for any person to "intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication."

46. "Intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

47. "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce."

48. In violation of 18 U.S.C. § 2511(1)(c), Defendants Del Rosso and Vital intentionally disclosed wire and electronic communications of Azima knowing and/or having reason to know that the information was obtained through interception.

49. Defendants Del Rosso and Vital directed CyberRoot to intentionally disclose large quantities of Azima's intercepted data by instructing that the data be posted on BitTorrent and WeTransfer. Links to those BitTorrent and WeTransfer sites were added to the blog sites that CyberRoot created. CyberRoot worked with BellTroX and at the direction of the Defendants to conduct the hacking and post the intercepted data. The BitTorrent and WeTransfer sites were posted by users named anjames and an_james, which are usernames associated with Sharma at CyberRoot. CyberRoot also used the email account an_james@protonmail.ch to create these blog sites and upload Azima's stolen data. The links were updated as recently as 2019.

50. The intercepted data included, among other things, business and personal electronic communications between Azima and others across the United States and around the world.

51. Defendants Del Rosso and Vital caused CyberRoot to hack Azima's computers and email accounts. The hack gave CyberRoot persistent access to Azima's computers and email accounts.

52. Defendants Del Rosso and Vital knew or had reason to know that the information published on the BitTorrent and WeTransfer sites was obtained through interception because Del Rosso and Vital gave the instructions to CyberRoot to intercept Azima's data and paid CyberRoot more than $1 million to conduct the hack and publish the stolen data. Defendants Del Rosso and Vital also knew or had reason to know that the information was obtained through interception because, among other reasons discussed above, it included large quantities of privileged, private, financially sensitive and trade secrets data, including private email communications, banking documentation, and business plans, including confidential internal pricing lists relating to food transport for U.S. troops in Afghanistan.

53. As a result of the disclosure of Azima's intercepted data, Azima suffered damages. Since at least June 2018, the stolen data has continued to be publicly available on WeTransfer through links that were posted to the blog sites created by CyberRoot, resulting in more than $75,000 of statutory damages under 18 U.S.C. § 2520(c)(2)(B), and further monetary damages in an amount to be proven at trial. Upon information and belief, Defendants Del Rosso and Vital have made significant profits from the disclosure of Azima's data, having been paid large sums of money to disclose the stolen data to damage Azima. As a result of the continued disclosure of Azima's stolen data, Azima has suffered,

and will continue to suffer, irreparable harm to his person, reputation, business, and community standing.

COUNT TWO (All Defendants)

II. Conspiracy to Disclose and Use Intercepted Wire, Oral, or Electronic Communications under the Wiretap Act (18 U.S.C. §§ 2511(1)(d) and 2520, 18 U.S.C. § 371)

54. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

55. Defendants Del Rosso and Vital willfully, intentionally, and knowingly agreed and conspired with CyberRoot, Dechert LLP, Page, and others to disclose Azima's intercepted data in violation of 18 U.S.C. §§ 2511 and 2520. Among other things, Defendants Del Rosso and Vital agreed and conspired to intercept Azima's data through a phishing and spear-phishing campaign resulting in the hackers obtaining persistent access to Azima's computers and email accounts. Defendants Del Rosso and Vital paid more than $1 million for the interception of Azima's data. Defendants Del Rosso and Vital also agreed and conspired to disclose the intercepted data by instructing CyberRoot to publish the data on blog sites that were created by CyberRoot. CyberRoot used BitTorrent and WeTransfer to send the stolen data to Defendants Del Rosso and Vital as well as other co-conspirators.

56. The BitTorrent and WeTransfer links were posted by users named anjames and an_james, which are usernames associated with Sharma at CyberRoot. Defendants also

used the email account an_james@protonmail.ch to create these blog sites and upload Azima's stolen data.

57. Defendants Del Rosso and Vital, with full knowledge that they were engaged in wrongful actions, took steps in furtherance of the conspiracy, including paying more than $1 million to the company that conducted the hacking, and later covering up the hacking through a story that the English court found to be false.

58. Azima has been injured and has suffered monetary damages as a result of Defendants' conspiratorial actions in an amount to be proven at trial. As a result of the Defendant's conspiracy to disclose and use Azima's intercepted data, Azima has suffered, and will continue to suffer, irreparable harm to his person, reputation, business, and community standing.

COUNT THREE (All Defendants)

III. Misappropriation of Trade Secrets, 18 U.S.C. §§ 1831, 1832, 1836

59. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

60. Federal law creates a cause of action against "[w]hoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly . . . steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains" trade secrets. 18 U.S.C. § 1832(a)(1).

61. Federal law imposes criminal penalties on "whoever . . . conspires with one or more other persons" to violate § 1832(a)(1). See § 1832(a)(5).

62. Federal law also creates a cause of action against "[w]hoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly – (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret." 18 U.S.C. § 1831(a)(1).

63. Federal law imposes penalties on "[w]hoever . . . conspires with one or more other persons to commit" the offense listed in § 1831(a)(1). See § 1831(a)(5).

64. "An owner of a trade secret that is misappropriated may bring a civil action . . . if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce." 18 U.S.C. § 1836(b)(1).

65. Azima's email accounts and computer systems stored trade secrets, including but not limited to highly confidential business plans and proposals, research supporting those plans and proposals (including costs and service projections), information concerning business strategies and opportunities, and contacts for important business relationships. These trade secrets are substantially valuable to Azima, in excess of $75,000, as will be proven at trial.

66. Azima stored trade secrets that were used in interstate and foreign commerce. Azima has taken and continues to take reasonable measures to keep this information secret.

For example, Azima has always maintained his information on secured servers that are protected by passwords, firewalls, and antivirus software.

67. Azima's trade secrets derive independent actual and potential economic value from not being generally known or available to the public or other persons who can obtain economic value from their disclosure or use.

68. Azima's trade secrets have significant value, resulting from substantial investment of time and resources.

69. Azima has made, and continues to make, efforts that are reasonable under the circumstances to maintain the secrecy of his trade secrets.

70. Defendants Del Rosso and Vital, along with CyberRoot, Dechert LLP, Page, and others, unlawfully conspired to take, appropriate, and obtain Azima's trade secrets without authorization, by means of a cyberattack against him. Defendants Del Rosso and Vital and their co-conspirators knew that Azima's email accounts contained trade secrets and intended to steal them in order to harm Azima.

71. Defendants Del Rosso and Vital improperly disclosed and misappropriated Azima's trade secrets without consent or authorization when they instructed CyberRoot to hack Azima, steal copies of his data, including trade secrets, and distribute the data through BitTorrent and WeTransfer links on blogs created by CyberRoot.

72. As a direct consequence of the unlawful actions of Defendants Del Rosso and Vital and their co-conspirators, Azima has suffered damages, which include, but are not limited to, loss of business goodwill, loss in the value of his trade secrets and

confidential business information, and harm to Azima's business, in an amount to be proven at trial. *See* 18 U.S.C. § 1836(b)(3)(B)(i)(I). Defendants' acts of misappropriation have affected interstate commerce.

73. As a direct consequence of the unlawful actions of Defendants Del Rosso and Vital and their co-conspirators, Defendants Del Rosso and Vital have unjustly benefited from their possession of Azima's trade secrets. Upon information and belief, Defendants Del Rosso and Vital, who were engaged by Dechert LLP, were paid substantial sums of money by Dechert LLP to conspire to steal and misappropriate Azima's trade secrets. Del Rosso and Vital in turn paid CyberRoot more than $1 million.

74. Defendants' conduct was willful and malicious.

COUNT FOUR (All Defendants)

IV. Computer Trespass (N.C. Gen. Stat. § 14-458)

75. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

76. In violation of N.C. Gen. Stat § 14-458, Defendants Del Rosso and Vital directly and/or through their agents knowingly and without authorization or reasonable grounds used Azima's computer and computer network with the intent to make or cause to be made unauthorized copies of Plaintiff's computer data.

77. Defendants had no right, authority, or permission to access or use Plaintiff's computer data or computer network.

78. Defendants Del Rosso and Vital conspired with others to use Azima's computer and computer network without authorization to make copies of Plaintiff's trade secrets, confidential business information, and personal information and communications that would provide Defendants and their co-conspirators leverage over Plaintiff.

79. Defendants Del Rosso and Vital instructed CyberRoot to hack Azima's computer and computer network and aided and abetted the hacking of Azima's computer data and computer network. At the direction of Defendants Del Rosso and Vital, CyberRoot, which worked with BellTroX, carried out the hack on Azima and gained access to Azima's computer and computer network. The breach of Azima's computer systems gave CyberRoot persistent access to Azima's email accounts and computers. Thus CyberRoot, acting at the direction of Defendants Del Rosso and Vital and others, regularly used Azima's computer and computer networks to make unauthorized copies of Azima's computer data, and Defendants Del Rosso and Vital caused these unauthorized copies to be made. Defendants Del Rosso and Vital paid CyberRoot more than $1 million for their hacking services.

COUNT FIVE (All Defendants)

V. Conversion (North Carolina Common Law)

80. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

81. Plaintiff was the lawful owner of his computer data and computer network, and was entitled to immediate and exclusive possession of his computer data and computer network.

82. Defendants directly and/or through their agents and co-conspirators, knowingly and without authorization or reasonable grounds, wrongfully possessed and converted computer data, documents, spreadsheets, communications, and other files owned by the Plaintiff.

83. Under North Carolina law, conversion occurs when a defendant wrongfully possesses or converts property under the ownership of the Plaintiff.

84. Defendants conspired to wrongfully obtain and exercise possession of Plaintiff's computer data, documents, spreadsheets, communications, and other files owned by the Plaintiff.

85. As discussed in more detail above, Defendants Del Rosso and Vital instructed CyberRoot to hack Azima and make unauthorized copies of Azima's computer data. At the direction of Defendants Del Rosso and Vital, CyberRoot successfully hacked Azima and converted Plaintiff's computer data by obtaining and utilizing persistent access to Azima's email accounts and computer systems. Thus CyberRoot, acting at the direction of Defendants Del Rosso and Vital and other co-conspirators, regularly accessed Azima's computer and computer networks to make unauthorized copies of Azima's computer data, and Defendants Del Rosso and Vital caused these unauthorized copies to be made.

Defendants Del Rosso and Vital paid CyberRoot more than $1 million for their hacking services.

COUNT SIX (All Defendants)

VI. Identity Theft (N.C. Gen. Stat. § 14-113.20 and § 1-539.2(c))

86. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

87. Defendants directly and/or through their agents and co-conspirators knowingly and without authorization or reasonable grounds, obtained, possessed, and used identifying information of Plaintiff with the intent to fraudulently represent that Defendants were the Plaintiff for the purposes of obtaining materials of value, benefit, and advantage.

88. Pursuant to N.C. Gen. Stat. § 14-113.20, "identifying information" is defined to include "passwords;" "electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names;" and "any other numbers or information that can be used to access a person's financial resources."

89. Defendants conspired with CyberRoot, Dechert LLP, Page, and others to obtain, possess, and use Plaintiff's identifying information – including electronic mail passwords – for the purposes of stealing and misappropriating trade secrets, confidential business information, and personal information and communications that would provide Defendants and their co-conspirators leverage over Plaintiff.

90. At the direction of Del Rosso, Vital, and others, CyberRoot sent Azima phishing emails asking him to reset his password. Azima complied, and unwittingly

permitted CyberRoot's hackers to gain access to Azima's email accounts and computers. The persistent access to Azima's email accounts and computers allowed CyberRoot, at the direction of Defendants Del Rosso and Vital, to use Azima's email addresses and passwords to obtain substantial quantities of Azima's private data, including trade secrets, confidential business information, and personal information and communications.

COUNT SEVEN (All Defendants)

VII. Publication of Personal Information (N.C. Gen. Stat. § 75-66)

91. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

92. Defendants knowingly broadcast or published personal information of Azima on the internet with actual knowledge that Azima objected to any such disclosure and without Azima's consent or knowledge.

93. Defendants published Azima's private information on blog sites hosting WeTransfer links in May and June of 2018, and again in June of 2019.

94. This personal information included, among others, checking account numbers, passwords, and other numbers and information that can be used to access Azima's financial resources.

95. Among other documents, Defendants published financial transaction records, spreadsheets, business records, and banking information, all of which were and are marked confidential.

96. Defendants' publication of Azima's personal information on the internet despite Azima's objection and without Azima's consent or knowledge directly and proximately caused actual injury to Plaintiff.

97. Defendants and their co-conspirators were not permitted, authorized, or required by any federal, State, or local law, regulation, or ordinance to access, collect, use, or release Azima's sensitive and confidential personal information.

98. At the direction of Del Rosso, Vital, and others, CyberRoot created blog sites accusing Azima of fraud. The blog sites contained links to BitTorrent sites that Dechert LLP later admitted contained large quantities of Azima's stolen data. These BitTorrent links were posted by users named anjames and an_james, which are usernames associated with Sharma at CyberRoot. CyberRoot also used the email account an_james@protonmail.ch to create these blog sites and upload Azima's stolen data. In May and June 2018, the blog sites were modified to include new links to WeTransfer sites that contained copies of Azima's stolen data CyberRoot regularly used WeTransfer links to transfer data to Vital. CyberRoot set up the WeTransfer account using the email account an_james@protonmail.ch.

99. During this same period, Del Rosso made significant payments to CyberRoot for their efforts.

100. Azima is entitled to damages for each of Defendants' unlawful acts of publication of personal information in accordance with N.C. Gen. Stat. § 1-539.2(c).

COUNT EIGHT (All Defendants)

VIII. Violation of Trade Secrets Protection Act (N.C. Gen. Stat. § 66-153 *et seq*.)

101. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

102. Azima's email accounts and computer systems contained business or technical information, formulas, patterns, programs, devices, compilations of information, methods, techniques, or processes. This information included highly confidential business plans and proposals, research supporting those plans and proposals (including costs and service projections), information concerning business strategies and opportunities, and contacts for important business relationships. This information constituted trade secrets under Chapter 66 of the North Carolina General Statutes.

103. Azima derived independent actual or potential commercial value from these trade secrets not being generally known or readily ascertainable through independent development or reverse engineering by persons who can obtain economic value from their disclosure or use.

104. Azima has undertaken and continues to undertake reasonable efforts under the circumstances to maintain the secrecy of his trade secrets. For example, Plaintiff has always maintained his information on secured servers that are protected by passwords, firewalls, and antivirus software.

105. Azima's trade secrets are substantially valuable to Plaintiff, in excess of $75,000, as will be proven at trial.

106. Azima kept trade secrets that were used in interstate and foreign commerce.

107. Azima's trade secrets have significant value, resulting from substantial investment of time and resources. If known to Azima's competitors, Plaintiff's trade secrets would be of value to those competitors.

108. Azima's trade secrets included, among others, confidential internal price lists and confidential spreadsheets connected to contracts with the United States government to supply troops in Afghanistan.

109. Defendants Del Rosso and Vital, along with CyberRoot, Dechert LLP, Page, and others, unlawfully conspired to acquire, disclose, or use Azima's trade secrets without express or implied authority or consent by means of a cyberattack against Azima. Defendants Del Rosso and Vital and their co-conspirators knew that Azima's email accounts and computer systems contained trade secrets and intended to steal them in order to harm Azima. Defendants did not arrive at Azima's trade secrets by means of independent development, reverse engineering, or by obtaining them from a person or entity with a right to disclose any of the trade secrets.

110. Defendants Del Rosso and Vital improperly acquired, disclosed, or used Azima's trade secrets without consent or authorization when they instructed CyberRoot to hack Azima, steal copies of his data, including trade secrets, and distribute the data through BitTorrent and WeTransfer links on blogs created by CyberRoot.

111. Defendants' conduct in acquiring, disclosing, or using Azima's trade secrets was willful and malicious and part of a deliberate, clandestine strategy and conspiracy to injure Azima.

112. Azima discovered that Defendants misappropriated his trade secrets earlier this year.

113. As a direct consequence of the unlawful actions of Defendants Del Rosso and Vital and their co-conspirators, Azima has suffered damages, including but are not limited to loss of business goodwill, loss in the value of his trade secrets and confidential business information, and harm to Azima's business, in an amount to be proven at trial. Defendants' acts of misappropriation have affected interstate commerce.

114. As a direct consequence of the unlawful actions of Defendants Del Rosso and Vital and their co-conspirators, Defendants Del Rosso and Vital have unjustly benefited from their possession of Azima's trade secrets. Upon information and belief, Defendants Del Rosso and Vital, who were engaged by Dechert LLP, were paid substantial sums of money by Dechert LLP to conspire to misappropriate Azima's trade secrets.

115. Del Rosso and Vital paid CyberRoot more than $1 million to conspire to misappropriate Azima's trade secrets.

116. Defendants' conduct in misappropriating Azima's trade secrets as described above directly and proximately caused actual injury to Azima.

117. Because Defendants' conduct was willful and malicious, Azima is entitled to punitive damages pursuant to N.C. Gen. Stat. § 66-154(c).

118. Because Defendants' conduct was willful and malicious, Azima is entitled to reasonable attorney's fees under N.C. Gen. Stat. § 66-154(d).

COUNT NINE (All Defendants)

IX. Unfair and Deceptive Trade Practices (N.C. Gen. Stat. § 75-1.1)

119. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

120. Defendants' conduct in sending Azima phishing and spear phishing emails in an effort to access and misappropriate his emails, computers, communications, confidential information, personal information, trade secrets, and other data constitutes an unfair and deceptive act or practice in violation of N.C. Gen. Stat. § 75-1.1.

121. Defendants' conduct in accessing Azima's emails, computers, communications, confidential information, personal information, trade secrets, and other data without his consent or knowledge constitutes an unfair and deceptive act or practice in violation of N.C. Gen. Stat. § 75-1.1.

122. Defendants' conduct in publishing or distributing Azima's emails, communications, confidential information, personal information, trade secrets, and other data on the internet constitutes an unfair and deceptive act or practice in violation of N.C. Gen. Stat. § 75-1.1.

123. Defendants committed conduct in or affecting commerce by (1) sending Azima phishing and spear phishing emails, (2) accessing Azima's emails, computers, communications, confidential information, personal information, trade secrets, and other

data without his consent or knowledge, and (3) publishing or distributing Azima's emails, communications, confidential information, personal information, trade secrets, and other data on the internet.

124. Defendants committed conduct that was unfair and deceptive by (1) sending Azima phishing and spear phishing emails, (2) accessing Azima's emails, computers, communications, confidential information, personal information, trade secrets, and other data, and (3) publishing Azima's emails, communications, confidential information, personal information, trade secrets, and other data on the internet.

125. Defendants' conduct in committing the unfair and deceptive acts or practices as described above was willful and malicious and part of a deliberate, clandestine strategy and conspiracy to injure Azima.

126. Defendants' conduct in committing the unfair and deceptive acts or practices as described above directly and proximately caused actual injury to Azima.

127. Plaintiff discovered that Defendants committed unfair and deceptive acts or practices that injured him on or about August 28, 2020 following an investigation.

128. Because Defendants' conduct constituted unfair and deceptive acts or practices under N.C. Gen. Stat. § 75-1.1, Plaintiff's damages should be trebled pursuant to N.C. Gen. Stat. § 75-16.

129. Because Defendants' conduct constituted unfair and deceptive acts or practices under N.C. Gen. Stat. § 75-1.1 and Defendants willfully and maliciously engaged

in that conduct, Plaintiff is entitled to recover reasonable attorney's fees pursuant to N.C. Gen. Stat. § 75-16.1.

COUNT TEN (All Defendants)

X. Civil Conspiracy (North Carolina Common Law)

130. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

131. Defendants and their co-conspirators CyberRoot, Dechert LLP, and others, knowingly and without authorization or reasonable grounds, wrongfully entered into an agreement to commit unlawful acts resulting in injury to Azima by conspirators pursuant to a common scheme of stealing Azima's confidential information to use against him.

132. Under North Carolina law, a civil conspiracy occurs when there is an agreement between two or more individuals to do an unlawful act or to do a lawful act in an unlawful way, resulting in injury to a plaintiff inflicted by one or more of the conspirators pursuant to a common scheme.

133. Under this agreement, Defendants directed that CyberRoot send phishing emails to induce Azima to reveal his credentials. Defendants would then use Azima's credentials to gain access to Azima's confidential information and copy the information for widespread publication. Defendants paid CyberRoot more than $1 million for these actions. Upon information and belief, Defendants were contracted and paid by Dechert LLP, on behalf of RAKIA, to conduct the hacking.

134. Because of Defendants' successful and unlawful phishing campaign against Azima, Azima had confidential information publicly exposed, suffered harm to business relationships, and suffered misappropriation of numerous trade secrets.

135. Defendants, CyberRoot, Dechert LLP, and Page engaged in this conspiracy pursuant to a common scheme of damaging Azima and tarnishing his reputation. Defendants are thus liable for the unlawful and tortious acts of all of the co-conspirators.

COUNT ELEVEN (All Defendants)

XI. Invasion of Privacy – Offensive Intrusion Upon Seclusion

136. Plaintiff incorporates by reference the allegations contained in the preceding paragraphs.

137. Defendants intruded upon Azima's privacy by invading his solitude, seclusion, private affairs and personal concerns.

138. Defendants invaded Azima's privacy intentionally because they knew that the hacking of Azima's email accounts and computer systems would intrude upon his privacy, or, at a minimum, Defendants acted with reckless indifference to the consequences of conspiring with Dechert LLP, CyberRoot, and other yet unknown co-conspirators to hack Azima's email accounts and computer systems.

139. Azima was and is highly offended by Defendants' intrusion upon his privacy, and any reasonable person would be highly offended under the same or similar circumstances. Azima reasonably expected that the highly confidential and sensitive

information, including confidential trade secrets, stored in his email accounts and computer systems would remain private.

PRAYER FOR RELIEF

On the basis of the foregoing, and such evidence as Plaintiff will present at trial, Plaintiff requests the entry of judgment in his favor and against Defendants on all counts of the Complaint and the award of the following relief:

1. Compensatory damages incurred by Azima as a result of the actions of Defendants, in an amount to be determined at trial.

2. Statutory damages, in an amount to be determined at trial, including treble damages and punitive damages.

3. A mandatory injunction requiring Defendants to remove and return of Azima's data from any computers, servers, or websites.

4. A prohibitory injunction obligating Defendants to refrain in the future from committing tortious acts against Plaintiff.

5. Pre-judgment and post-judgment interest in the amounts and at the rates provided by law.

6. Costs and expenses, including reasonable attorney's fees, incurred by Plaintiff in this action and as a result of the actions of Defendants alleged herein.

7. Such other and further relief as the Court deems just and proper.

JURY DEMAND

Plaintiff Farhad Azima respectfully requests a trial by jury of all issues so triable.

This, the 15th day of October, 2020.

Respectfully submitted,

WOMBLE BOND DICKINSON (US) LLP

/s/ Jonathon Townsend
Jonathon D. Townsend
North Carolina 51751
Christopher W. Jones
North Carolina Bar No. 27625
Ripley Rand
North Carolina Bar No. 22275
555 Fayetteville Street, Suite 1100
Raleigh, North Carolina 27601
Phone: 919-755-2100
Fax: 919-755-2150
Email: jonathon.townsend@wbd-us.com
ripley.rand@wbd-us.com
chris.jones@wbd-us.com

MILLER & CHEVALIER CHARTERED

/s/ Kirby D. Behre
Kirby D. Behre (*pro hac vice forthcoming*)
Brian Hill (*pro hac vice forthcoming*)
Tim O'Toole (*pro hac vice forthcoming*)
Ian Herbert (*pro hac vice forthcoming*)
Calvin Lee (*pro hac vice forthcoming*)
900 16th Street, NW
Washington, D.C. 20006
Telephone: (202) 626-5800
Fax: (202) 626-5801
Email: kbehre@milchev.com

Counsel for Plaintiff